Your response

We welcome the opportunity to respond to the Consultation, ‘Protecting people from illegal harms online’.

Question (Volume 2)	Your response
Question 6.1: Do you have any comments on Ofcom’s assessment of the causes and impacts of online harms? Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.	*[Is this answer confidential? Yes /* ***No*** *(delete as appropriate)]* 1) One area that we think is not adequately mentioned up front, is the fact that 30% of all users online are minors. Whilst in the offline world, it is relatively easy to know when you are dealing with a child, and to estimate the approximate age of the child and adapt accordingly - this has not been the default online. Currently, the age of the user is not known in most online settings. This is vital for any analysis of the causes and impacts of online harms. Hence it should be the first question which is asked. Currently it is not addressed explicitly in this Volume. If it could be added, that would provide useful context for measures recommended later in the document. 2) In general, we note that preventative safety tech measures could assist in supporting the outcome of safety by design. Currently the focus of the OSA appears to be on measures to ‘take down’ rather than measures to prevent harms such as NCII, CSAM or to optionally verify users which could reduce the workload for NGOs and law enforcement. Hopefully this is something that Ofcom will consider and redress the balance to make services safer overall. It would be tragic for the end result of the act to become an auditing tick box exercise.

Question (Volume 2)	Your response
Question 6.2: Do you have any views about our interpretation of the links between risk factors and different kinds of illegal harm? Please provide evidence to support your answer.	*[Is this answer confidential? Yes /* ***No*** *(delete as appropriate)]* Ofcom's guidance and public stance of 'ensuring that the burden on smaller or less-resourced businesses is not disproportionate' appears to be skewed to interpret that smaller or less-resourced businesses should be exempt from preventing illegal harm. Would the same logic apply in other sectors, where health and safety of consumers is paramount; that the cost of doing business should not require investment in solutions to keep consumers safe? Should the size of the organisation be measured or rather the risks assessed in terms of 4Cs - content, conduct, contact, contract to minors?

Question (Volume 3)	Your response
Question 8.1: Do you agree with our proposals in relation to governance and accountability measures in the illegal content Codes of Practice? Please provide underlying arguments and evidence of efficacy or risks to support your view.	*[Is this answer confidential? Yes /* ***No*** *(delete as appropriate)]* No We agree that either a named person or an overall governance body should carry out an annual review to record how the service has managed the risk of illegal harms. Large organisations identified with a specific risk should undertake Internal monitoring and assurance to assess the effectiveness of measures to mitigate and manage the risks of harm, reporting to a governance body or an audit committee. This should be straightforward for any large organisation which will generally have an internal audit function in place. **However, we disagree** again with the argument that there should be a differential burden and treatment for large versus small organisations, where smaller startups 'might not be expected to implement as many of the recommended mitigations'. Safety tech providers have built solutions which can be easily integrated by large or small organisations in just a couple of hours. Neither the cost or effort are out of reach for small organisations. The requirement for smaller and larger organisations to use

Question (Volume 3)	Your response
	safety tech to comply with regulation will encourage more competition between safety tech suppliers ensuring services are affordable.
Question 8.2: *Do you agree with the types of services that we propose the governance and accountability measures should apply to?*	*[Is this answer confidential? Yes /* **No** *(delete as appropriate)]* No. We disagree in a number of areas: We think that it would be preferable to extend monitoring and assurance to all services with specific risks, not just the largest platforms.. In particular we suggest that protections from grooming should be applied to all sites, not only those which already do age assurance as this creates a perverse incentive not to assure age. We suggest that there is a rephrasing to "means of knowing users are under 18" rather than the term 'identifying' which has other connotations. We suggest that Ofcom should set out the range of ways by which sites may already know or suspect that users as under 18 (self-declaration, profiling or marketing, research findings, evidence of the age of users on similar sites) We would ask Ofcom to extend adult user controls to all users, including children, by default. Given the importance of prevention, we would ask Ofcom to require processes to detect new CSAM, for all sizes of sites. We ask Ofcom to require age assurance for performers to preventing underage performers - on all sizes of sites; not just the largest platforms. We would ask Ofcom to explicitly state how it will work across the eco system to extend its support and education to all sizes of platforms. We would like to see transparency as to how Ofcom is working in conjunction with payment processors [1]and advertising networks - given the adage 'follow the money' - in order to really bring to bear the spirit of the Online Safety Act in full and make it a level playing field across all organisations.

[1] https://segpay.com/MC_RevisedStandardsForNewSpecialtyMerchantRegistrationRequirementsForAdultContentMerchants.pdf

Question (Volume 3)	Your response
Question 8.3: Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to requiring services to have measures to mitigate and manage illegal content risks audited by an independent third-party?	*[Is this answer confidential? **No]*** Yes We would advocate that the internal audit functions of large organisations which may own many titles or sub brands, as well as regulators themselves, and payment processors and ad networks can deploy supervisory technology to assess if appropriate and effective measures are in place. We are aware and have shared with Ofcom, details of services to scan for compliance, which are available and accessible to all organisations in the ecosystem. We support the mention of the trusted, independent third parties for auditing age assurance solutions, such as the Age Check Certification Scheme (ACCS). There are parallel United Kingdom Accreditation Service (UKAS) accredited audit bodies in the UK which certify providers for other frameworks, such as the Digital Identity & Attributes Trust Framework. It is important that, in time, there is a healthy ecosystem of audited providers and UKAS accredited audit bodies, or audit bodies accredited by other regulators. Market forces will support competitive pricing in terms of audit. We would like to see Ofcom and other regulators becoming more active in the field of mutual recognition of international certification and international standards, such as those being developed by the IEEE and ISO. This could be a topic for consideration by the Global Online Safety Regulators Network and the international working group across data protection regulators. For instance, Yoti has been approved during a lengthy process by two regulators the FSM and KJM, over a couple of years, by the ACCS and the NCC Group in the UK, as described in the paragraphs below. The KJM for instance has recently undertaken more research into minimum standards for data minimised age checks, requiring specific stages to be undertaken. It would be useful for all involved that minimum standards and audit processes can be understood by other nations; rather than every country replicating the same due diligence. This is also cost prohibitive for smaller nations and also for new and emerging age assurance providers. It will make it harder for platforms to comply and it will also decrease investment in the safety tech sector if multiple audits and standards apply across the world. To illustrate the range of audits & benchmarks that we have engaged with so far: Yoti's age estimation technology has been approved for the highest level of age assurance by the German regulator Kommission für

Question (Volume 3)	Your response
	Jugendmedienschutz (KJM) (or *'Commission for the Protection of Minors in the Media'*). The KJM has a decade of experience of reviewing over 100 approaches for age assurance (https://www.kjm-online.de/aufsicht/technischer-jugendmedienschutz/unzulaessige-angebote/altersverifikationssysteme) and and its approval of facial age estimation, can be found on the KJM website: https://www.kjm-online.de/service/pressemitteilungen/meldung/kjm-bewertet-yoti-age-scan-als-technisches-mittel-positiv. Yoti's liveness detection technology was also reviewed by the United States' National Institute of Standards and Technology (NIST). Yoti's 'MyFace' technology was awarded 'iBeta NIST Level 2' with 100% attack detection rate by NIST in 2023. Yoti's liveness detection and penetration resistance technologies are also independently assessed in the context of Yoti's certification to the UK digital identity and attributes trust framework (UKDIATF). Yoti has submitted its facial age estimation algorithm to the NIST global benchmark. [2] Yoti has been reviewed by ACCS and previously NCC Group, on behalf of the BBFC. Yoti's facial age estimation has been certified since 2020 by the Age Check Certification Scheme for use in a Challenge 25 policy area. The intention of the test is to assess whether or not the Yoti Age Estimation System is fit for deployment by determining if an 18 year-old (the nominal age) would be incorrectly estimated as being over 25 (the Challenge Age policy). The ACCS report stated: *'The report highlights how, subject to the exclusions mentioned in the report, our testing indicates that this version of the tool PASSES for deployment in a Challenge 25 policy area.'* Even 4 years ago in 2020, the system was *'deemed fit for deployment in a Challenge 25 policy area and at least 98.89% reliable*. The report also said: *'The Yoti AI Services Age API version 1.1.1 (Target of Evaluation) assessed on or before 17th November 2020 can be stated to accurately estimate the age of person of nominal age 18 as being under the age of 25 with 98.89% reliability where results are stated by the Yoti system to an uncertainty of less than 4.6 years.'* The mean absolute error, mean predicted age, upper and absolute tolerances were all within the permitted parameters as set out in ACCS 1:2020 Technical Requirements for Age Estimation Technologies. In addition, at the request of one of our clients, our May 2022 white paper was independently verified by the ACCS for our measurement methodology

[2] https://pages.nist.gov/frvt/html/frvt_age_estimation.html

Question (Volume 3)	Your response
	and accuracy of our results. The ACCS said that: “*The training, testing and results reporting presented in the Yoti white paper have been independently validated by ACCS, who have certified that Yoti have deployed appropriate methodologies to analyse the performance of their Facial Age Estimation algorithm, including ensuring appropriate separation of machine learning training data, testing data and validation data.*”
Question 9.2: Do you think the four-step risk assessment process and the Risk Profiles are useful models to help services navigate and comply with their wider obligations under the Act?	*[Is this answer confidential?* ***No****]* Whilst we are generally supportive of the methodology for service risk assessments provided in this documentation, we would like to repeat the point made throughout our response that Ofcom should always make it clear that service providers should never be encouraged to verify the **full date of birth** of their users and keep a record of that unless other, more privacy-preserving age solutions are available and adapted. Indeed, as the documentation states, the Online Safety Act regime is fundamentally reliant on age thresholds (for example 18, 16, and 13 years of age), and therefore the need for providers should only be to ascertain whether individuals are **above or below such thresholds.** Where for user-to-user and search service providers the text in *‘Volume 3: The causes and impacts of online harm’* says ‘*We will guide all services to consider the following evidence when doing their risk assessment: Risk Profiles (and relevant parts of Ofcom’s Register of Risks), user reports, user complaints, user data including age (where relevant), retrospective analysis of incidents of harm and other relevant information that a service holds*’. We recommend that Ofcom should make it clear that the evidence that is necessary to effectively conduct a risk assessment is **not** the exact date of birth or age of a user. Rather, it is sufficient and better from a privacy point of view for users to focus on establishing whether their users fall above or under a threshold. *‘Annex 5: Service Risk Assessment Guidance.’* We would recommend, in *‘Table 10. Core evidence inputs’* (*‘Where relevant, user data including age’*) that Ofcom makes clear that it does not recommend that providers retain the information resulting from an age assurance or age verification step taken by a user other than to assign a user to an age threshold. This annex document should make very clear that providers must take a proportionate approach to age data collection and retention. We would welcome more information about A5.127 and A5.128, particularly in the case of smaller providers who may not have in-house horizon scanning functions.

Question (Volume 3)	Your response
	We would also like to see more information as to how Ofcom will communicate with providers about the changes it may make to the *'Risk Profiles'*. We would suggest that such communications should not be restricted solely to in-scope providers but be made available to the whole online safety ecosystem. We also regret to see that self-assessment criteria such as the ease of circumvention of measures and the evolution of circumvention techniques (for example virtual private networks or 'VPNs'), and users' literacy levels in that field seem to have been left out of the documentation, aside from a duty on providers not to promote them on their site. We think these are important factors to consider when assessing and implementing an age assurance solution and suggest that they should be included in the guidance. Given that OFCOM has significant experience of dealing with VPNs in other areas of its regulatory remit; we would recommend a proactive stance, to explains how it already works directly with ISPs in terms of VPNs in other contexts and to combat url hopping, for instance its work with regards dynamic injunctions for sports betting. Sites should check the age of individuals who use VPNs to discourage children from trying to evade being age checked by using VPNs.
Question 9.3: Are the Risk Profiles sufficiently clear and do you think the information provided on risk factors will help you understand the risks on your service?[3]	*[Is this answer confidential? **Yes**]* [✂]

[3] If you have comments or input related to the links between different kinds of illegal harm and risk factors, please refer to Volume 2: Chapter 5 Summary of the causes and impacts of online harm).

[4] https://carnegieuktrust.org.uk/blog-posts/bringing-small-high-harm-platforms-into-the-online-safety-bill/

Question (Volume 3)	Your response
Question 10.1: Do you have any comments on our draft record keeping and review guidance?	*[Is this answer confidential?* ***No****]* The key element should be public transparency in terms of record keeping by content platforms; so that this can be scrutinised by regulators and civil society. Platforms should offer their users a choice of methods and providers of IDV, including third party options. We would repeat that Ofcom to make it clear in the *'Scope of our proposed guidance'* text, and in particular in footnote 157 in relation to point 10.5, that in the interest of privacy Part 5 providers should solely retain metadata about a check meeting the level of assurance required and that they may not keep a record of a user's full date of birth). We would also suggest a clarification of the wording of the duty for service providers to *'keep a durable written record of the age assurance process in use'* that is '*up-to-date and easy to understand*', which we see as an improvement but also still potentially misleading. We understand that it should be possible for providers to employ *'alternative measures'* to demonstrate compliance with the regime as described in the *'Records of alternative measures taken to comply with a relevant duty'* in '*Annex 6: Guidance on record keeping and review*'. However, we would invite Ofcom to require providers who implement *'alternative measures'* of age assessments to have these methods independently assessed such as for accuracy, false positives, false negatives, inclusivity and ease of circumvention. We would highlight the need 1) for regulators to assess the transparency and require independent review to assess the origin of AI datasets, bias levels and the accuracy of artificial intelligence approaches and 2) also a clear expectation for businesses to undertake effective supplier due diligence as to the legality of their training data capture, meeting GDPR, and data practices. We would also like to see the outcome of those assessments to be in a format similar to the guidance and assessments that Ofcom will make and publish with regards to the more common forms of age assurance currently used by the industry.

Question (Volume 4)	Your response
Question 11.1: Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?	*[Is this answer confidential?* ***Yes]*** [✂]

Question (Volume 4)	Your response
Question 11.2: Do you agree that in general we should apply the most onerous measures in our Codes only to services which are large and/or medium or high risk?	[Isthisanswerconfidential?**Yes**/No(deleteasappropriate)] [✂]
Question 11.3: Do you agree with our definition of large services?	*[Is this answer confidential? **Yes** / No (delete as appropriate)]* [✂]
Question 11.6: Do you have any comments on the draft Codes of Practice themselves?[8]	*[Is this answer confidential? **Yes** (delete as appropriate)]* [✂]

[8] See Annexes 7 and 8.

Question (Volume 4)	Your response
Question 11.7: Do you have any comments on the costs assumptions set out in Annex 14, which we used for calculating the costs of various measures?	*[Is this answer confidential?* ***No*** *(delete as appropriate)]* We question as to why there is no inclusion of costing of preventative measures for CSAM in terms of costs? (e.g. there is a section 'Further analysis on CSAM hash matching measures'..as though this was the only possible approach) It is worth considering the costs for law enforcement and civil society will continue to spiral, if preventative measures are not deployed across the ecosystem, with regulators working in conjunction with payment processors and ad networks as well as platforms. We provide a link here to rate card levels of e signatures as just one example of an approach that can support content uploaded to adult content platforms is given with consent and by an adult and that co performers in content are also over 18 and have given consent. We provide a link to our blog where we mention the free offer of the Yoti reusable digital identity app, for sharing a data minimised 18 plus attribute; from within the Yoti Age Verification Service (AVS), where we offer a range of age assurance services. We would ask Ofcom to look at tokenised approaches to age assurance and to work with co regulators in the Global Online Safety Regulators Network and across the EU to consider interoperable, tokenised approaches. This requires some very basic reflection as to how long should a token last in certain contexts; eg. for access to adult content. Despite the fact that the OSA mandates Category 1 services to provide adult users with controls for specific types of content and includes the ability to filter out non-verified users. This implies that Category 1 services must offer all adult users the option to verify their identity. It is stated that the verification process can use any method and doesn't necessarily require documentation. However, there seems to be no costing or further detail provided as to verification options; which is very peculiar.

Question (Volume 4)	Your response
	We would ask Ofcom to engage with DSIT and the 40 plus organisations which are certified as identity providers under the Digital Identity & Attributes Trust Framework, for the current specific use cases. There is a vibrant ecosystem of organisations which could support in terms of offering consumers a choice of verification approaches, for the online verification duty, which consumers could choose to use if they so decide. Bodies such as techUK, the APPG Digital Identity and Open Identity Exchange could support the convening of organisations to suggest a range of approaches for the optional verification duty.
Question 12.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	[Is this answer confidential? **Yes** / No (delete as appropriate)] [✂]

Question (Volume 4)	Your response
Question 13.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? **Yes** / No (delete as appropriate)]* [✂]

Question (Volume 4)	Your response
Question 14.1: Do you agree with our proposals? Do you have any views on our three proposals, i.e. CSAM hash matching, CSAM URL detection and fraud keyword detection? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? Yes /* **No** *(delete as appropriate)]* We do not think the approaches should be limited to three take down proposals, as detailed above, there should be equal focus on preventative measures. We are concerned OFCOM has not yet gained sufficient understanding to recognise that unintentional unconsented publication; of genuine porn, or deep fake lookalike porn, can be prevented using existing safety tech and this safety tech is already 'in market'.
Question 15.1: *Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.*	*[Is this answer confidential?* ***No****].* No We strongly disagree that these takedown measures alone will be effective. We would invite Ofcom to look at other prevention techniques currently available. We also fear that the focus is just on the largest platforms; when a level playing field is needed. The harms do not only manifest in large platforms. Safety tech approaches can serve all sizes of organisations. *As per the government Safety tech sector analysis report*[12]*,* *There are now over 115 safety tech businesses based in the UK…These are essential technologies in the fight against online*

[12] https://assets.publishing.service.gov.uk/media/62e2b66c8fa8f5032b58ce3e/OS0057_UK_Safety_Tech_Analysis_2022_Online_v4__2_.pdf

Question (Volume 4)	Your response
	harms, and they ensure that a wide range of digital platforms have the tools they need to keep their users safe online.
Question 18.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? **No**]* We welcome the inclusion in this document of recommendations to use age assurance technologies (*'Where services are already using age assurance technologies, they should use these to determine whether someone is a child for the purposes of the protections set out below'*), however regret the suggestion that other providers may resort to using the outcome of self-declarations *'for the time being'*. We would repeat the need for a speedier delivery of the roadmap (*'Ofcom's approach to implementing the Online Safety Act'*) to regulation, particularly on age assurance. As we have said previously, we would recommend in section 18.78 that Ofcom make it clear that there are a range of age assurance approaches, and that consumers should be offered choice. For instance, age estimation does not require an individual to submit any personal information. And that where identity documents are an option; there are selective disclosure approaches offered by third party age verification providers, so that just the over 18 or over 13 attribute is shared with the relying party, rather than the full *'photo-ID document'*. Moreover, these measures have different resistance levels to circumvention attempts. It is indeed easier to take a parent's credit card to circumvent a credit card-based check, than it is to procure sophisticated masks or artificial intelligence technology. Therefore, we think Ofcom should undertake research to assess the ease of circumvention of the full range of age assurance approaches. We also believe that self-declaration should not be included in this section nor the wider guidance and that Ofcom should, like the global online safety community has in recent years, recognise that self-declaration is not fit for purpose and that providers should in no way rely on the age data acquired through it. Indeed that is the case of Ireland's national online safety regulator, the Coimisiún na Meán, which states in its latest 'Draft Online Safety Code' consultation that 'mere self- declaration of age is not regarded as an effective age verification technique'. This opinion is also shared by the Netherlands' national online safety regulator, the *Commissariaat voor de Media* (*'we think that self-declaration is not an appropriate age-verification tool,' 'Responses to Coimisiún na Meán Call for Inputs: Online Safety Code'*). Therefore we disagree with 18.80, and believe self-declaration should be ruled out. We would point out that the data quoted in

Question (Volume 4)	Your response
	18.79 from the *'Children's Online User Ages Quantitative Research Study'* piece (*'a third of respondents aged 8-17 who had a social media profile were pretending to be aged 18 or over'*) could underestimate the true proportion of false self-declarations. Given the recruitment of child respondents for this study was via their parents and the data was collected through a survey, also on the basis of self-declaration - it is very likely that fewer respondents would admit to lying about their age, if their continued access to that service could be affected. There is significant risk that OFCOM's expert judgement will be damaged if it allows sites to place reliance on age historically, or in future, ascertained through self-declaration. Finally, a point that we will repeat throughout the documentation is the need for independent third party auditing and benchmarking of the effectiveness of age assurance solutions in order to help better guide relying parties when they look to put in place measures to mitigate the harms arising from their risk assessments. Indeed, whilst very large platforms may have the resources to conduct internal studies into each type of age assurance technology, this will not be true for the overwhelming majority of providers.
Question 19.3: We are aware of design features and parameters that can be used in recommender system to minimise the distribution of illegal content, e.g. ensuring content/network balance and low/neutral weightings on content labelled as sensitive. Are you aware of any other design parameters and choices that are proven to improve user safety?	*[Is this answer confidential? Yes /* ***No*** *(delete as appropriate)]* Again we would encourage Ofcom to consider upstream what can be done to deter illegal / CSAM content to be uploaded from the outset, how to gather consent and ensure uploading is only possible from adults and that all individuals in content are over 18 and have provided consent. We would ask Ofcom to review the outcomes of the government funded Safety tech Challenge Fund[13]: 1. Yoti joined forces with video and image moderation company DragonflAI to create a solution that instantly detects a person's age in explicit content on a device and completely offline. 2. Yoti partnered with end-to-end email encryption platform Galaxkey, and content analysis platform Image Analyzer to innovate a messaging platform that detects explicit content before it is sent, rather than after the fact.

[13] https://www.yoti.com/blog/safety-tech-challenge-fund-2021/

Question (Volume 4)	Your response
Question 21.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential?* ***No****]* 1) '*Verifying users' identity*': we were surprised to read the section below: *In vol 4, 21.7 While we do not propose to recommend identity verification in our Codes for illegal harms, we note that, under the Act, 'Category 1 services' have an additional specific duty to offer optional identity verification as a user empowerment tool. We will issue guidance in respect of the user empowerment duty for Category 1 services in later phases of our work.* We would encourage Ofcom to bring forward this work and to engage with the vibrant digital identity verification provider community in the UK to develop clear guidelines. Yoti is a provider of identity verification technology ('IDV') that has been independently assessed for accuracy when it became the first identity service provider (IDSP) to be certified to the United Kingdom Digital Identity & Attributes Framework (UKDIATF). Currently, the guidance does not require IDV technology providers to have any certification, and so less robust technologies, together with the ease with which fake identity documents can be procured in the UK today, can severely undermine the level of age or identity assurance provided by IDV technology. Therefore, we would recommend that Ofcom recommend providers in scope of the regime use a certified IDSP only, and further that they specify minimum standards of verification so as to add the highest level of trust and assurance to the whole technological supply chain. For instance, a document upload, without liveness detection, face matching or a document authenticity check would not achieve a high level of assurance. At the time of writing, there is a very healthy ecosystem of providers certified to the trust framework, to support this. 2) '*Verifying users' age*': We welcome the addition of a recommendation '*to use proportionate systems and processes*'. We believe that this should be repeated throughout the document. We would suggest a rewording of *'requiring users to verify their age has the potential to prevent children from being exposed to other illegal harms'* to read *'requiring the implementation of age assurance helps prevent children from being exposed to other illegal harms'*.

Question (Volume 4)	Your response
	This is again because we do not believe verifying the full age of users is proportionate in all circumstances, where either the selective disclosure of an age attribute or facial age estimation could provide a quicker, less disruptive and more privacy-preserving solution. This must be made clear throughout the guidance. To the point raised in 21.108 (‘*There are a range of age assurance techniques available which are capable of achieving varying degrees of accuracy and effectiveness*’), we would repeat that we would like to see age assurance techniques independently assessed. We will continue to support Ofcom's work in this field.
Question 21.2: Do you have any supporting information and evidence to inform any recommendations we may make on blocking sharers of CSAM content? users.	*[Is this answer confidential?* **No** *(delete as appropriate)]* As mentioned above, as a provider of identity verification and age assurance approaches, we would be happy to engage with Ofcom to re outline measures : -to ensure that those uploading content are over 18 and that all performers are over 18 and provide consent. -to provide a range of approaches for optional or platform mandated verification - to support content moderation
Question 22.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? No (delete as appropriate)]* No; again we reiterate our recommendation that the focus should shift to prevention, rather than solely take down.
Question 23.1: Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?	*[Is this answer confidential?* **No** *(delete as appropriate)]* No, we disagree, as outlined above.

Question (Volume 4)	Your response
Question 23.2: Do you agree that the overall burden is proportionate for those small and micro businesses that find they have significant risks of illegal content and for whom we propose to recommend more measures?	*[Is this answer confidential? Yes /* ***No*** *(delete as appropriate)]* No, we disagree., as outlined above.
Question 23.3: We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?	*[Is this answer confidential? Yes /* ***No*** *(delete as appropriate)* No, as previously outlined, we would advocate that there should be a level of playing field of measures.
Question 24.1: Do you agree that Ofcom's proposed recommendations for the Codes are appropriate in the light of the matters to which Ofcom must have regard? If not, why not?	*[Is this answer confidential?* ***Yes****]* [✂]

Question (Volume 4)	Your response

Question (Volume 5)	Your response
Question 26.1: Do you agree with our proposals, including the detail of the drafting? What are the underlying arguments and evidence that inform your view.	*[Is this answer confidential? Yes /* ***No*** *(delete as appropriate)]* As mentioned several times above, we do not think that solely 3 measures for automated content detection (hashing, url detection, keyword search) are sufficient in terms of the minimum requirement, as they come downstream, after content is published.
Question 26.2: Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?	*[Is this answer confidential? Yes /* ***No*** *(delete as appropriate)]* The size of the guidance makes it very challenging for all but the largest of organisations who are blessed with large dedicated legal and policy teams.
Question 26.3: What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?	*[Is this answer confidential?* ***No****]* We would like to make some comments about *'Annex 10: Online Safety Guidance on Judgment for Illegal Content'*. We acknowledge this is a very sensitive and difficult topic, and base our feedback on our own experience. We have some reservations about the methodology proposed in A4.31 and A4.33, particularly around the suggestion that providers should *'make a common-sense judgement as to whether the subject of the image is under 18'*. We would draw Ofcom's attention to the 'Report Remove' tool implemented by the National Society for the Prevention of Cruelty to Children (NSPCC)'s Childline counselling service.

Question (Volume 5)	Your response
	More information about this tool as well as the importance and ramifications of establishing whether a person is over or under 18 in those circumstances are available at: https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/report-remove/. Similarly, we have reservations about the current drafting of A5.16 and A5.17.

Question (Volume 6)	Your response
Question 28.1: Do you have any comments on our proposed approach to information gathering powers under the Act?	*[Is this answer confidential?* ***No****]* Our general feedback to the proposed information gathering powers approach is that we would like to see more transparency, such as by publishing information notices and information requests made by Ofcom and requests that are to do with technologies such as age assurance used by providers (as per 28.7 d)). We would welcome more clarity about whether Ofcom would include age assurance technology providers in the scope of their notices, and if so under what time constraints. We would encourage Ofcom in conjunction with partner regulators around the world, to liaise with open banking and mobile phone operators to understand what role they can play to support the activities of age assurance; what is the quality of their datasets in terms of knowing who is an adult and who is a minor and to consider how reauthentication could uplift existing datasets. We would also ask Ofcom to work widely in the online ecosystem; including liaising with payment processors and ad networks to widen the range of organisations which can support its supervision and regulatory activities. *'Information notices'*: As per 28.7 g), we would encourage Ofcom to bring forward the target date for the publication of the *'Report on age assurance technologies'* that is currently scheduled for Q3 2026 in *'Figure 2: Our timeline for online safety implementation'* of '*Ofcom's approach to implementing the Online Safety Act.*' *'Skilled person report'*: We believe the current wording of 28.23 ('*who appears to us to have the skills necessary'*) remains too ambivalent and subjective. We would also welcome the inclusion of a transparency element over the appointment of *'skilled persons'* to undertake the review of a provider's duty, so as to provide an understanding of how Ofcom has assessed that their skillset matches the inspection need. *'Disclosure of Information'*: Our general feedback to this section is that we would encourage Ofcom to be as transparent as possible about its enforcement

Question (Volume 6)	Your response
	activities and in particular auditing albeit without revealing sensitive commercial information. We think it important to help the public understand what Ofcom is doing to foster a feeling that the Online Safety regime is adopted and fit for purpose. We would welcome more detail as to how Ofcom will assess the different parameters mentioned in 28.46 and when a decision is made not to *'disclose confidential information'* as under 28.48. We would welcome more information on whether Ofcom intends to make public its *'reasoning and approach'* as under 28.53, and whilst we recognise the list provided in 28.55 is non exhaustive, we would welcome the inclusion of a pathway for members of the public and users to submit evidence to support Ofcom's work.
Question 29.1: Do you have any comments on our draft Online Safety Enforcement Guidance?	*[Is this answer confidential?]* ***Yes*** [✂]